Rules and regulations regarding student use of Stockholm University (SU) computers, network and system facilities

Background

These regulations are based on the fact that all computing, facilities, networks, affiliated equipment and accounts owned and operated by Stockholm University (SU) are for use in such activities and operations as are sanctioned by SU. All other activities, such as personal development are permissible only when such activities:

- do not disturb normal university usage
- do not violate or conflict with departmental rules, SU regulations, SUNET (Swedish University Network) regulations, or any applicable laws.

For the purpose of these rules a user is defined as any SU student who has benn allocated an account or received permission to use SU computing facilities, network or system resources.

Authorization

- An account an the resources allocated to it may only be used by the authorized account holder.
- The password connected to the authorization must not be disclosed to anyone. In exceptional cases this may be done to the head of the department or unit. Detailed information regarding the use and management of passwords is available in computer-readable form at www.su.se and can also be obtained from the computer security officer or the systems administrator at each department or unit. The account holder is responsible for staying informed about and complying with all rules governing password use.
- All certified accounts have a specified time limit and will be closed upon termination of the authorized user's studies. Except by special agreement, SU reserves the right to close an account when the user account has been inactive for more than six months.

Utilization

- All use of Su's computer facilities for commercial purposes is strictly prohibited unless permission is specifically granted for said purposes.
- SU equipment may not be used to view, download, print or in any other way handle or disseminate pornographic or offensive material.
- Account users are not permitted to deliberately conceal their user identity when using the computer network and associated resources, except in those cases where special permissions has been granted by the Vice-Chancellor of Stockholm University or is a consequence of informant freedom or other statutory right stemming from the principle of public access to official records.

- Exploitation of defective configurations, program errors or other means of securing a higher level of privilege than authorized by the system personnel is strictly prohibited.
- SU is no way liable for the functioning or the accessibility of its systems.
- General copying and distribution are permitted only when the original clearly states in writing that material may be disseminated. Material protected by copyright may only be copied and distributed after written permission has been received from the copyright owner. Copyright-protected music and films may not be downloaded, nor may copyright-protected music, films and computer programs be copied onto CD's, DVD's, disks or any other storage medium, from any source whatever. Please note that special rules apply to the use and storage of personal information.
- Pursuant to Swedish law, SU is responsible for taking measures against the publication and distribution of certain types of material.
- Anyone who detects violations of these rules or regulations, such as illegal activities, errors or flaws in the system, or any other irregularities or problems, shall immediately report said violations or problems to both the departmental system administrator and the computer security officer.
- Users are specifically requested to take notice of Swedish laws strictly forbidding the persecution of ethnic groups, as well as prohibitions against sabotage, damaging or disruptive activities directed against SU facilities or other users, and unauthorized access or attempts to gain unauthorized access in local SU systems external to SU.

Enforcement

Some of the information available on the SU computer network is to be regarded as public documents and thereby subject to Swedish laws on public access to official records.

Please note that such information may have been illegally manipulated.

- It is the responsibility of the computer security officer/system administrator to maintain control over the SU computer network and to take all measures necessary to ensure such control. However, this must not be done in such a manner as to hinder the individual freedom to publish, inform, debate, or exercise other statutory rights according to the principle of public access to official records.
- SU is legally responsible for the removal of all criminal information from the SU computer network.

Additional points

All computer security officers and system administrators shall report any breach of these rules and regulations and/or applicable laws to the head of the department or unit.

In accordance with the legislation for public employment, the Vice-Chancellor decides whether such a report shall be referred to the student disciplinary board or forwarded for prosecution. All other cases that may require further measures of technical administrative nature are referred to the Technical Support Division for decisions such as closing the user's account or terminating user access to computer, network and system resources, or any other appropriate measures pending further investigation. Such administrative actions must not interfere with the student's studies, except in consequence of disciplinary action by the appropriate authority.

SU retains written agreements with computer security officers and system administrators regarding the treatment of the information that they gain access to on SU networks. Should suspicion of crime be involved, other rules may apply.

Copies of these rules and regulations shall be available at all departments and units as well as in computer-readable form as www.su.se